



9110-9P

**DEPARTMENT OF HOMELAND SECURITY**

**[Docket ID DHS-2018-0019]**

**The President's National Security Telecommunications  
Advisory Committee**

**AGENCY:** National Protection and Programs Directorate,  
Department of Homeland Security.

**ACTION:** Committee management; notice of federal advisory  
committee meeting.

**SUMMARY:** The President's National Security  
Telecommunications Advisory Committee (NSTAC) will meet on  
Thursday, May 17, 2018, in Washington, DC. The meeting  
will be partially closed to the public.

**DATES:** The NSTAC will meet on Thursday, May 17, 2018, from  
9:30 a.m. to 3:30 p.m. Eastern Time (ET). Please note that  
the meeting may close early if the committee has completed  
its business.

**ADDRESSES:** The May 2018 NSTAC Meeting will be held at the  
Eisenhower Executive Office Building, Washington, DC. Due  
to limited seating, requests to attend in person will be  
accepted and processed in the order in which they are  
received. The meeting's proceedings will also be available  
via Webcast at <http://www.whitehouse.gov/live>, for those  
who cannot attend in person. Individuals who intend to

participate in the meeting will need to register by sending an email to [NSTAC@hq.dhs.gov](mailto:NSTAC@hq.dhs.gov) by 5:00 p.m. ET on Friday, May 11, 2018. For information on facilities or services for individuals with disabilities, or to request special assistance at the meeting, or to attend in person, contact [NSTAC@hq.dhs.gov](mailto:NSTAC@hq.dhs.gov) as soon as possible.

Members of the public are invited to provide comment on the issues that will be considered by the committee as listed in the **SUPPLEMENTARY INFORMATION** section below. Associated briefing materials that participants may discuss during the meeting will be available at [www.dhs.gov/nstac](http://www.dhs.gov/nstac) for review as of Friday, May 4, 2018. Comments may be submitted at any time and must be identified by docket number DHS-2018-0019. Comments may be submitted by one of the following methods:

- **Federal eRulemaking Portal:**

<http://www.regulations.gov>. Please follow the instructions for submitting written comments.

- **Email:** [NSTAC@hq.dhs.gov](mailto:NSTAC@hq.dhs.gov). Include the docket number DHS-2018-0019 in the subject line of the email.
- **Fax:** (703) 705-6190, ATTN: Sandy Benevides.
- **Mail:** Helen Jackson, Designated Federal Officer, Stakeholder Engagement and Critical Infrastructure Resilience Division, National Protection and Programs

Directorate, Department of Homeland Security, 245

Murray Lane, Mail Stop 0612, Arlington, VA 20598-0612.

Instructions: All submissions received must include the words "Department of Homeland Security" and the docket number DHS-2018-0019. Comments received will be posted without alteration at [www.regulations.gov](http://www.regulations.gov), including any personal information provided.

Docket: For access to the docket and comments received by the NSTAC, please go to [www.regulations.gov](http://www.regulations.gov) and enter docket number DHS-2018-0019.

A public comment period will be held during the meeting on Thursday, May 17, 2018, from 2:40 p.m. to 3:00 p.m. ET.

Speakers who wish to participate in the public comment period must register in advance by no later than Friday, May 11, 2018, at 5:00 p.m. ET by emailing [NSTAC@hq.dhs.gov](mailto:NSTAC@hq.dhs.gov).

Speakers are requested to limit their comments to three minutes and will speak in order of registration. Please note that the public comment period may end before the time indicated, following the last request for comments.

**FOR FURTHER INFORMATION CONTACT:** Helen Jackson, NSTAC

Designated Federal Officer, Department of Homeland

Security, (703) 705-6276 (telephone) or

[helen.jackson@hq.dhs.gov](mailto:helen.jackson@hq.dhs.gov) (email).

**SUPPLEMENTARY INFORMATION:** Notice of this meeting is given under the Federal Advisory Committee Act, 5 U.S.C. Appendix (Pub. L. 92-463). The NSTAC advises the President on matters related to national security and emergency preparedness (NS/EP) telecommunications and cybersecurity policy.

Agenda: The committee will meet in an open session on May 17, 2018, receive remarks from Department of Homeland Security (DHS) leadership and other senior Government officials regarding the Government's current cybersecurity initiatives and NS/EP priorities. The meeting will include a keynote address and a debate consisting of great thinkers in cybersecurity. NSTAC members will also receive a status update on the NSTAC Cybersecurity Moonshot Subcommittee's examination of concepts related to a Cybersecurity Moonshot, which has two primary objectives: (1) defining an ambitious but achievable outcome-focused end goal for the cybersecurity environment; and (2) defining the structure and process necessary to successfully execute against the identified end goal.

The committee will also meet in a closed session to receive a classified briefing regarding cybersecurity threats and discuss future studies based on the Government's NS/EP priorities and perceived vulnerabilities.

Basis for Closure: In accordance with 5 U.S.C. 552b(c), The Government in the Sunshine Act, it has been determined that two agenda items require closure, as the disclosure of the information discussed would not be in the public interest. The first of these agenda items, the classified briefing, will provide members with a cybersecurity threat briefing on vulnerabilities related to the communications infrastructure. Disclosure of these threats would provide criminals who seek to compromise commercial and Government networks with information on potential vulnerabilities and mitigation techniques, weakening the Nation's cybersecurity posture. This briefing will be classified at the top secret/sensitive compartmented information level, thereby exempting disclosure of the content by statute. Therefore, this portion of the meeting is required to be closed pursuant to 5 U.S.C. 552b(c)(1)(A) & (B). The second agenda item, a discussion of potential NSTAC study topics, will address areas of critical cybersecurity vulnerabilities and priorities for government. Government officials will share data with NSTAC members on initiatives, assessments, and future security requirements across public and private sector networks. The information will include specific vulnerabilities within cyberspace that affect the United States' information and

communications technology infrastructures and proposed mitigation strategies. Disclosure of this information to the public would provide criminals with an incentive to focus on these vulnerabilities to increase attacks on the Nation's critical infrastructure and communications networks. As disclosure of this portion of the meeting is likely to significantly frustrate implementation of proposed DHS actions, it is required to be closed pursuant to 5 U.S.C. 552b(c) (9) (B) .

**Helen Jackson,**

*Designated Federal Officer for the NSTAC.*

[FR Doc. 2018-09234 Filed: 4/30/2018 8:45 am; Publication Date: 5/1/2018]